DATA AUTHENTICATION DEMONSTRATION FOR RADIONUCLIDE STATIONS

Mark Harris and Pres Herrington, Sandia National Laboratories
Harry Miley, J. Edward Ellis, David McKinnon, and Devon St. Pierre, Pacific Northwest National Laboratory

Sponsored by U.S. Department of Energy
Office of Nonproliferation and National Security
Office of Research and Development
Contract No. DE-AC04-94AL85000

ABSTRACT

Data authentication is required for certification of sensor stations in the International Monitoring System (IMS). Authentication capability has been previously demonstrated for continuous waveform stations (seismic and infrasound). This paper addresses data surety for the radionuclide stations in the IMS, in particular the Radionuclide Aerosol Sampler/Analyzer (RASA) system developed by Pacific Northwest National Laboratory (PNNL).

Radionuclide stations will communicate data by electronic mail using formats defined in IMS 1.0, Formats and Protocols for Messages. An open message authentication standard exists, called S/MIME (Secure/Multipurpose Internet Mail Extensions), which has been proposed for use with all IMS radionuclide station message communications. This standard specifies adding a digital signature and public key certificate as a MIME attachment to the e-mail message. It is advantageous because it allows authentication to be added to all IMS 1.0 messages in a standard format and is commercially supported in e-mail software. For command and control, the RASA system uses a networked Graphical User Interface (GUI) based upon Common Object Request Broker Architecture (CORBA) communications, which requires special authentication procedures.

We have modified the RASA system to meet CTBTO authentication guidelines, using a FORTEZZA card for authentication functions. We demonstrated signing radionuclide data messages at the RASA, then sending, receiving, and verifying the messages at a data center. We demonstrated authenticating command messages and responses from the data center GUI to the RASA. Also, the particular authentication system command to change the private/public key pair and retrieve the new public key was demonstrated. This work shows that data surety meeting IMS guidelines may be immediately applied to IMS radionuclide systems.

Key Words: authentication, radionuclide

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

OBJECTIVE

All monitoring stations in the International Monitoring System (IMS) must include data authentication equipment before certification [1]. Authentication technology has previously been demonstrated for seismic and infrasound stations [2], and is becoming commercially available. Authentication has not yet been implemented on radionuclide station hardware. This work was conducted to clarify the specifications issued by the PTS and demonstrate the feasibility of implementing data and command authentication at radionuclide stations.

RESEARCH ACCOMPLISHED

The protocols used within the IMS for radionuclide data use the standard Internet electronic mail system for delivery. Radionuclide data is formatted as text messages as specified in IMS 1.0 [3] and simply emailed to its recipient. With the global computer network capability available today, this has proven to be a flexible and powerful data communication mechanism, as is evidenced by the success of AutoDRM systems for waveform data retrieval. Basing user protocols upon standard industry protocols also allows commodity software products to be used for at least some elements of the system, reducing development cost.

Building upon this, the PTS has specified that radionuclide data messages should be authenticated using protocols of the Secure/Multipurpose Internet Mail Extensions (S/MIME) [4]. S/MIME is a developing standard of the Internet Engineering Task Force (IETF) S/MIME working group [5], which has been widely adopted in industry. S/MIME specifies procedures for signed and/or encrypted data and X.509 public key certificates to be transmitted as MIME attachments [6]. Feghhi et al. [7] thoroughly describes the complexities of using digital certificates and the associated public-key infrastructure (PKI) in the Internet environment. The overall key management structure needed for the use of public key certificate technology by the IMS has been addressed in previous demonstrations and is well understood [2,4]. Note that with this technology, all public key information needed to verify digital signatures is embodied within X.509 certificates.

Other PTS authentication specifications are also required for radionuclide stations. Briefly, these specify that all IMS data must be signed at the stations and all commands generated remote from the station must be verified. The Digital Signature Standard (DSS) [8] must be used, with public key size of 1024 bits. The signature function must be performed in a dedicated, tamper indicating hardware device. This device must be capable of self-generating a private key and communicating the new public key. The system must also support a remote key change command with transmission of the new public key to IMS authorities.

A hardware cryptographic token that meets these PTS requirements has been used in previous demonstrations. This token (the U.S. Government developed Fortezza Card) isolates cryptographic operations and private key material on a PCMCIA processor card. At least one company (SPYRUS, http://www.spyrus.com/) now offers a Fortezza-compatible card with only authentication functions installed, making it free of U.S. export restrictions on strong encryption.

Many commercial products support the S/MIME standards employed here (to varying degrees, since some parts of the current standards are considered drafts and are actively being developed). Conformance to S/MIME is generally good enough so that various commercial and open source products work together reliably. This is a great advantage, as it limits the extent of custom software that must be developed and distributed to the community. Any user with access to the certificates distributed by the IDC can verify signatures on data using a standard electronic mail software package, such as *Netscape Messenger*.

A radionuclide monitoring station: RASA

To investigate the feasibility of implementing data and command authentication at a radionuclide monitoring station, we have developed a demonstration of this technology using the PNNL-developed RASA station equipment (see Figure 1). The RASA provides ultrasensitive field measurement of short-lived fission products in near real time. This permits detection at great distances from nuclear detonation sites. The analyzer passes air through a large-area, low-pressure-drop filter at a high flow rate for selectable time periods; then seals, barcodes and performs a gamma-ray analysis of the filter. The gamma-ray spectrum is automatically transmitted to appropriate organizations. Filter samples are retained for subsequent analysis. The RASA operates automatically and all functions are remotely programmable. The RASA is now being manufactured commercially.

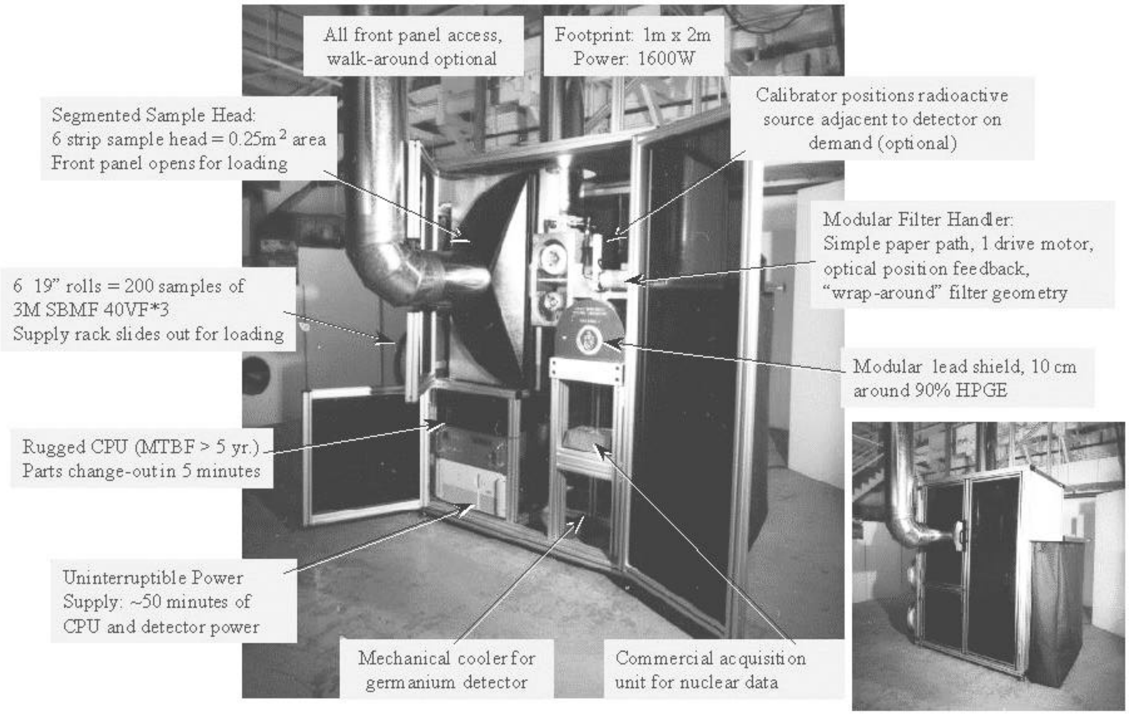
All front panel access, walk-around optional
Footprint: 1m x 2m Power: 1600W
Segmented Sample Head: 6 strip sample head = $0.25m^2$ area Front panel opens for loading
Calibrator positions radioactive source adjacent to detector on demand (optional)
Modular Filter Handler: Simple paper path, 1 drive motor, optical position feedback, "wrap-around" filter geometry
6 19" rolls = 200 samples of 3M SBMF 40VF*3 Supply rack slides out for loading
Modular lead shield, 10 cm around 90% HPGE
Rugged CPU (MTBF > 5 yr.) Parts change-out in 5 minutes
Uninterruptible Power Supply: ~50 minutes of CPU and detector power
Mechanical cooler for germanium detector
Commercial acquisition unit for nuclear data

Figure 1. RASA radionuclide monitoring equipment.

Authentication software developed

To support this demonstration, the prototype RASA system at PNNL was modified to perform authentication functions internally. A PC Card reader was integrated into the computer system within the RASA so that a Fortezza card could be installed. The standard driver software for the Fortezza card (the CI Library) was ported to the operating system of the RASA computer. This allowed software that already uses the Fortezza card with CI Library to be easily ported and used on the RASA.

We have adapted the *authd* software, used in past authentication demonstrations, to run on the RASA computer. This authentication server program manages interactions with a Fortezza card and maintains a database of public key certificates for use in verifying signed messages. Applications connect to *authd* using a socket interface and can request signature and verification operations on blocks of data. Standard key management issues may also be handled using this interface, such as requesting a new key pair be generated. We extended *authd* to perform tasks related to message authentication: X.509 certificate handling and PKCS #7 signature generation [9]. The OpenSSL software package [10] is used as the basis library for certificate processing. An *authd* client library is provided so that operations may be easily integrated into other software applications.

For this demonstration a system was assembled to simulate all relevant components of the IMS: the radionuclide station itself, a receiving data center, and certification equipment used by a PTS Key Management Authority. This system is illustrated here and described below.

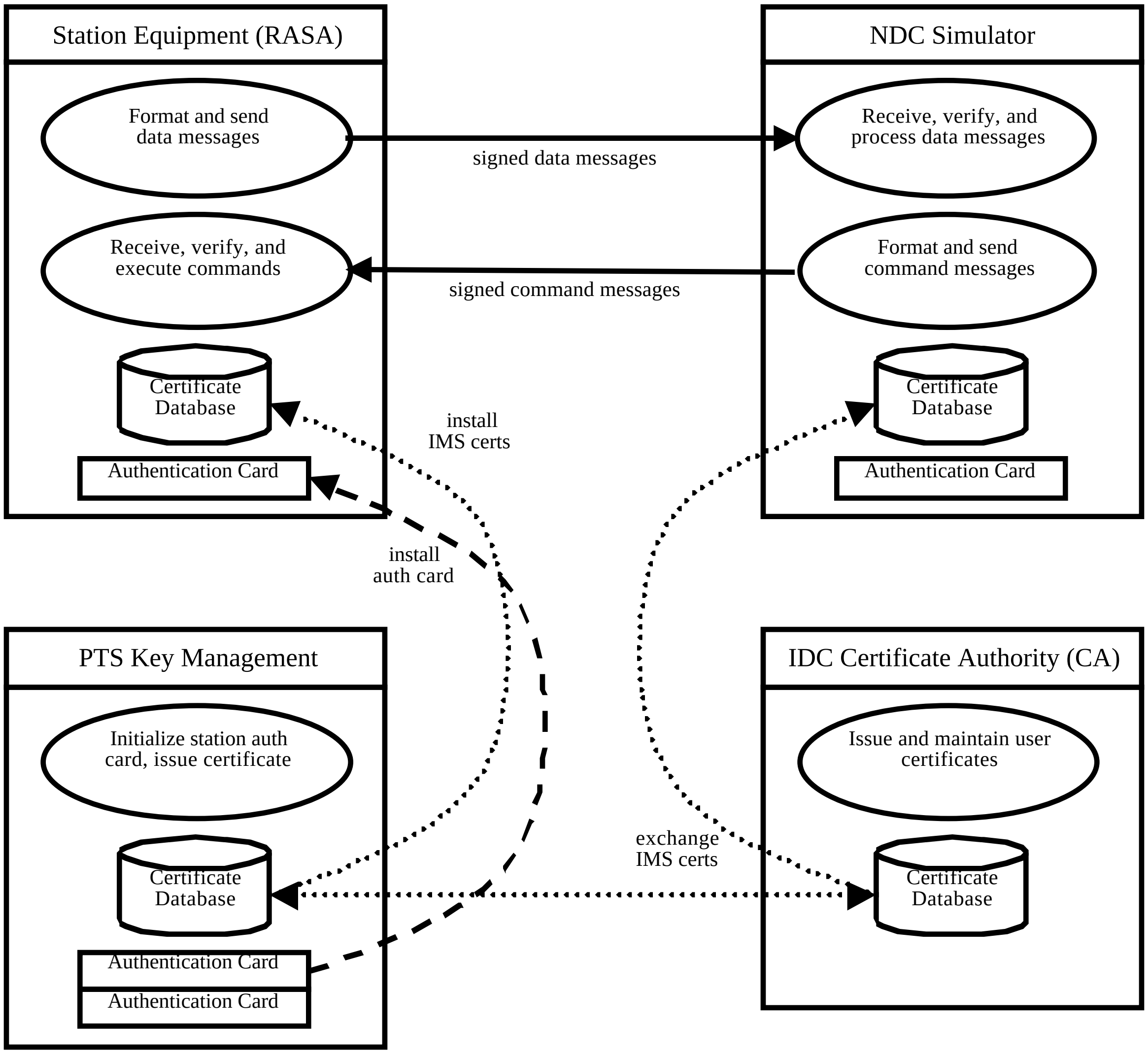

Figure 2. Demonstration system overview.

A realistic procedure was developed to initialize the authentication unit and install public keys at the station. This simulates the actions performed by a PTS Key Management Authority (also referred to as a certification observer) during an initial IMS certification visit. This initial secure transaction is the basis of trust for the station from that point on. The observer certifies that the public key information obtained for the station is trustworthy by issuing the station public key certificate and signing it. The observer further certifies that the public keys for remote users of the station are securely installed. After this transaction, authenticated messages may be transmitted between station and data center on an open network and reliably verified, until some event (such as tampering at the station) breaks the chain of trust.

For this demonstration, a certificate authority (CA) was simulated for the IDC using functions in OpenSSL. The CA serves as the root of trust in PKI systems, and must be administered in a very secure manner (security of the CA is not addressed here). The CA certifies all user certificates (either by signing them directly or indirectly) and distributes them to other users. Users can load these certificates into their message authentication software (e.g. *authd* or *Netscape*). Users need the certificate of the CA (and any indirect authorities) to verify messages under this structure. In the case of this demonstration, the simulated IDC CA certifies the observer, which certifies the station. Initially, users need both the CA and observer public-key certificates to authenticate the station certificate. Once the station certificate has been securely transmitted to the CA by the observer, the CA may certify it directly and distribute it to users.

To support standard message data authentication, S/MIME formatting software was developed and integrated into the RASA data processing flow (see Figure 3). Since radionuclide stations already use email messages, formatting and transmission capabilities were already available. An extra step was introduced to take each standard email message and convert it to an S/MIME message with attached digital signature calculated by the authentication card. The *authd* program creates a standard PKCS #7 signedData attachment, including the X.509 certificate for the station, which contains the public key. Then the S/MIME format data message is sent to the recipient in the usual way (in this case to the NDC Simulator). Normally the message would be automatically verified and processed at the data center. For this demonstration we simply view the message and verify the signature in *Netscape*.

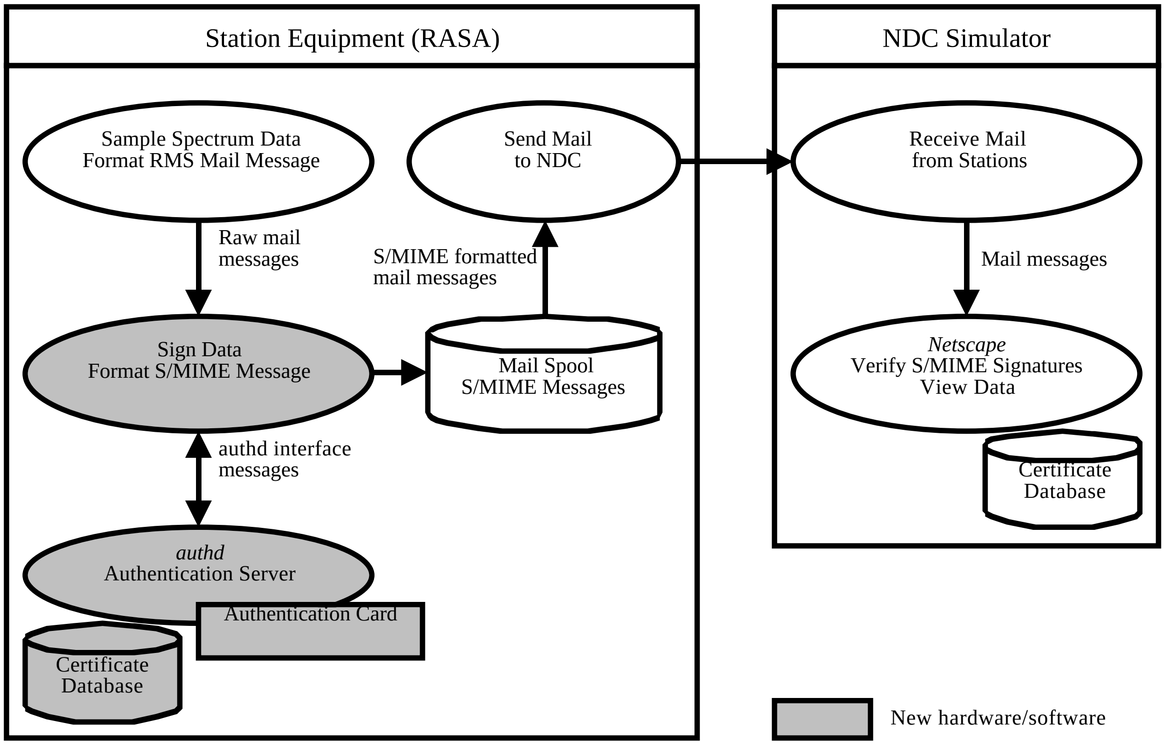

Figure 3. Data authentication flow diagram.

Originally, software for remote command and control of the RASA equipment was tightly integrated between the client (remote user) and server (RASA computer) software. This type of communication is difficult to operate in a highly secured manner on an open network (though some products are becoming available to secure individual TCP/IP connections end-to-end on a network that could be applied here). To illustrate command authentication with the RASA, a new command mode was developed which limits communications to discrete signed and verified transactions. Again, *authd* is used for authentication functions (see Figure 4). S/MIME format is used for the command message signatures in this demonstration. Two commands are demonstrated: a command to generate an interim spectrum measurement and a command to change the key pair on the authentication unit within the RASA. The first command results in a data message being generated and sent from the RASA in the usual manner. The second command causes the authentication software in the RASA to generate a new key pair in the authentication card, generate a new X.509 public key certificate (signed using the original key), and forward this new certificate to recipients as part of the next data message.

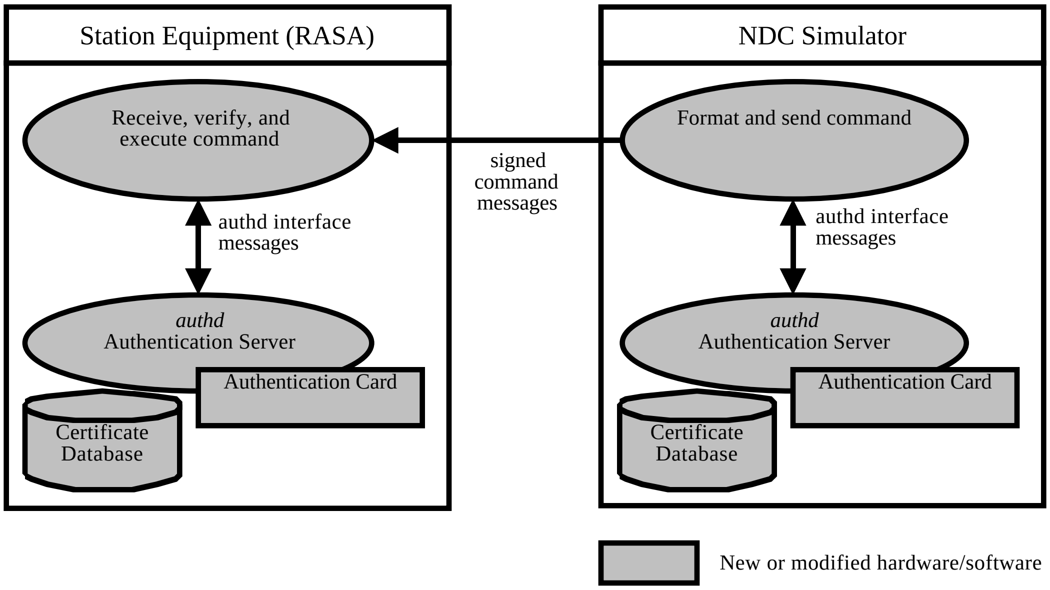

Figure 4. Command authentication flow diagram.

Authentication operations demonstrated on the RASA

We conducted a demonstration of all aspects of data surety at a radionuclide station: system initialization and key management, data authentication using S/MIME messages, and remote command authentication. The procedures used in this demonstration are summarized here.

Initialization operations at the IDC for the PTS Key Management Authority (the observer) were:
1. Obtained an authentication unit (e.g. a hardware authentication card).
2. Initialized authentication unit, generate a new key pair and public key certificate.
3. Certified public key certificate with IDC certificate authority (CA).
4. Obtained relevant public key certificates (for remote command users) for distribution to the station.

Initialization operations at the station were:
1. Observer obtained the station authentication card.
2. Observer initialized the authentication card with standard parameters and instructed it to generate a new key pair.
3. Observer generated a public key certificate for the authentication card and signed it with his own private key. The observer is known as the issuer of the station certificate. [At this point a chain of trust exists from the IDC CA through the observer to the station authentication unit.]
4. Observer installed the authentication card in the station equipment.
5. Observer installed relevant public key certificates (IDC, NDC, and station) in the station equipment.
6. Station began using new private and public keys.
7. Observer securely transferred new station certificate to the IDC for certification and distribution.

During normal operation, a radionuclide station periodically transmits a data message to the receiving data center. Once the station authenticator is initialized, all data and status messages are signed. The procedure for demonstrating this function was:
1. Wait to receive email data or status messages from the station on the NDC Simulator.
2. View the messages on the NDC Simulator (using Netscape), noting the status of the signature verification.

- Note that public key certificates must be installed into Netscape for the IDC CA and the observer that issued the station certificate.

Command authentication involves sending signed command messages from the NDC Simulator to the station:

1. Format a command message on the NDC Simulator.
2. Send the command message to the RASA.
3. RASA software verifies the message signature and completes the command.
4. In the case of the Key Change command, after the key pair has been changed by *authd* and a new certificate generated, an email message is queued to be signed and sent to the standard recipients, in order to propagate the new public key.

CONCLUSIONS AND RECOMMENDATIONS

We have demonstrated authentication technology for radionuclide stations using the required formats and protocols. Industry standards have been followed, allowing this system to work with existing software products. The demonstrated system should meet IMS certification requirements for authentication, and will be further developed and integrated into the RASA system for operational use.

This work is also applicable to other parts of the IMS where message authentication is needed. In particular, auxiliary seismic stations that use an email-based AutoDRM data communication method could use the demonstrated hardware and software to provide authenticated data transmission to the IDC. Automated signature verification on incoming data could be performed using this software, though performance limits of the hardware authentication card could be restrictive. The IDC itself (as well as the NDCs) could adapt this software to provide authenticated data products to users. Once the required certificate management system is in place signature verification will be available for all data users.

Some operational issues were not known while this demonstration was being prepared, and should be addressed if they have not been already. For example, the S/MIME protocol is flexible with regard to the number and details of the certificates that are attached to the signature. These details should be specified to ensure compatibility of software throughout the IMS and IDC.

REFERENCES

1. *Procedures for IMS Station Certification*, CTBT/PTS/INF.144/Rev.1, 13 May 1999.

2. Draelos, T., M. Harris, P. Herrington, and D. Kromer, Data Surety Demonstrations, *20th Seismic Research Symposium on Monitoring a CTBT*, September 1998.

3. *Formats and Protocols for Messages – IMS 1.0*, IDC-3.4.1Rev1, March 1999.

4. *Task Leader Paper on Authentication*, CTBT/WGB/TL-6/4/Rev.4, 12 February 1999.

5. S/MIME Working Group, http://www.imc.org/ietf-smime/, 1999.

6. Galvin, J., S. Murphy, S. Crocker, and N. Freed, *Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted*, RFC 1847, October 1995.

7. Feghhi, J., J. Feghhi, and P. Williams, Digital Certificates: Applied Internet Security, Addison Wesley Longman, 1999.

8. *Digital Signature Standard (DSS)*, FIPS PUB 186, 1994.

9. Kaliski, B., *PKCS #7: Cryptographic Message Syntax Version 1.5*, RFC 2315, March 1998.

10. OpenSSL: The Open Source toolkit for SSL/TLS, http://www.openssl.org/, 1999.